Solicitor General Canada | Solliciteur général Canada

Public Advisory: Special Report on Africa-Related E-Mail Solicitations

Summary

The Department of the Solicitor General of Canada and the United States Department of Justice are jointly issuing a Special Report to advise the public not to respond to e-mail solicitations (or similar letter or fax solicitations) that purport to come from individuals living or working in Africa, or to send or give money or their financial account information to anyone who contacts them in connection with such solicitations. If you have lost funds as a result of these solicitations, or have other questions concerning these solicitations, please contact the authorities listed below in this Advisory.

Facts

In recent months, law enforcement agencies and residents throughout North America have reported a significant increase in the number and variety of e-mail solicitations that purport to come from individuals living or working in Africa. E-mails – as well as letters and faxes -- of this type are commonly known as "Nigerian scam letters" or "4-1-9 schemes" (referring to the Nigerian criminal code provision for fraud) because they have been associated with criminal organizations that were based in Nigeria or consisted mainly of persons of Nigerian origin.

- In the initial versions of these e-mails, the senders falsely stated that they were associated with the "Nigerian National Petroleum Corporation" or other government agency in Nigeria. They allegedly had identified certain contracts that had been "over-invoiced" by tens of millions of dollars. The senders also represented that they needed the e-mail recipient's help in transferring the funds from these contracts to foreign bank accounts. In return, they promised the recipient a substantial percentage of the funds for assisting in the transfer.

- Invariably, however, recipients who agreed to cooperate have been defrauded out of large amounts of money – in some cases, hundreds of thousands or even millions of dollars – by entrusting their personal or business bank account information, or by sending the funds directly, to participants in the transaction.

More recent e-mails of this type now purport to come from persons not only in Nigeria, but from other nations in central and southern Africa, such as the Ivory Coast, Sierra Leone, South Africa, Togo, and Zimbabwe. Although these e-mails often seem to be personally addressed to the recipients, they are typically sent in massive quantities of unsolicited e-mail ("spam"), from Web-based e-mail accounts that people can quickly establish with little or no verification of their true identities and physical locations. By using Web-based e-mail accounts, criminals can check their accounts, and send follow-up e-mails to anyone who responds favorably to the initial solicitations, from anywhere in the world without disclosing their true locations.

Moreover, these more recent e-mails are using a wider variety of "pitches" – fraudulent stories explaining the need for the recipient's assistance. Although these e-mails uniformly appear fraudulent, many of them include general references to real historical events to make the "pitch" more plausible.

Here are some of the more frequently reported solicitations:

- *The "Air Crash Victim" Pitch*
  In these e-mails, the sender falsely represents himself to be an official or employee of a bank in Nigeria. He states that a foreign national had died in an airplane crash but had left a substantial account in that bank with no known next-of-kin.
    - For example, in one of the e-mails, the "bank official" states that an Australian national, "Butch R. Miguel," who had left an account with his bank containing U.S. $15.5 million, had died "three years ago in a ghastly air crash in an Egypt Air, Flight 990 which occurred on 2nd November 1999." (In fact, on October 31, 1999, an EgyptAir Flight 990 crashed in the Atlantic Ocean off Nantucket Island, Massachusetts, resulting in the deaths of all 217 passengers and crew and the destruction of the aircraft. There were, however, no Australian nationals and no one named either Butch or Miguel among the passengers on Flight 990.)
    - In a similar e-mail, the bank official asserts that a German national who had left U.S. $41 million in an account with his bank, had died along with his wife, in the recent plane crash involving Concord AF4590 in Gonesse, France." (In fact, on July 25, 2000, Air France flight 4590 crashed in Gonesse, France, killing 133 persons, including two people with German names similar to the names used in the e-mail).

- The "bank official" asserts that the decedent's funds, absent a next-of-kin, will be put to some other use by his bank.
- In the case of "Mr. Miguel," the "official" stated that his management had decided that Miguel's funds "be declared 'un-claimable" and subsequently be donated to the Trust Fund for the purchase of arms and ammunition to further enhance the course of war in Africa and the world."
- In the case of "Mr. Schinister," the "official" said that his management would "declare the deceased account dormant and revert the funds to trading on behalf of and in the interest of the Bank."
- The "bank official" therefore seeks the recipient's help in pretending to be the decedent's next-of-kin so that he can transfer the funds into the recipient's account. The recipient is promised 20 percent of the funds, but must provide the location and account number of his bank for the transfer.

- *The "Auditor General of Prime Banks" Pitch*

In these e-mails, the sender falsely represents himself to be the "Auditor General of Prime Banks" in Africa. He states that he is seeking to transfer tens or hundreds of millions of dollars overseas from a "prime bank." (In fact, there is no such office in any African nation, as courts and law enforcement and regulatory agencies have recognized that there is no such thing as a "prime bank." Many fraud schemes offer investments in nonexistent "prime bank" instruments.)

- The "Auditor General" also states that the funds are in the account of a deceased foreign individual, and that the money is not in local currency and can be transferred only to a foreigner with a foreign bank account.
- The "Auditor General" then typically offers the recipient a fee of 35 percent of the total funds at the conclusion of the transaction. He also requests that the recipient send back his or her private telephone and fax number, "including the full details of the account to be used for the deposit."

- *The "Widow and Orphan" Pitch*

In these e-mails, the sender represents himself or herself to be the widow, son, or daughter of a person who has died under tragic circumstances, typically at the hands of hostile government forces.

- One e-mail, supposedly from a resident of Zimbabwe, reported that "my father was one of the best farmers in the country and knowing that he did not support the president's political ideology, the president's supporters invaded my father's farm and burnt down everything, killed him and confiscated all his investments." (In fact, diplomatic reports have noted that Zimbabwe continues to have incidents of land seizures and political violence.)

- The sender then explains that he or she had to move for reasons of

personal safety, but had hidden away several millions, or tens of millions, of dollars from the hostile government forces, and now needed the help of a foreigner to transfer the money to a safe location outside of Africa.

- In the Zimbabwe letter described above, the sender claimed that he and his mother had sought asylum in South Africa, but that as asylum-seekers they could not open a non-resident bank account there.
- The sender typically urges the recipient to respond by e-mail or to a telephone number included in the e-mail.

In addition, the e-mails typically insist on absolute secrecy by the recipient, but promises that the transaction will be completely "risk-free." In the end, the recipient who responds favorably runs an extremely high risk of loss.

Advice

The Department of the Solicitor General of Canada and the United States Department of Justice are hereby advising the public not to respond to e-mail solicitations (or similar letter or fax solicitations) of this type, or to send or give money or their financial account information to anyone who contacts them in connection with such solicitations. If you have lost funds as a result of these solicitations, or have other questions concerning these solicitations, please contact the following authorities:

Canada

Phonebusters National Call Center
E-Mail: info@phonebusters.com
Telephone [Toll-Free]: 1-888-495-8501
Fax [Toll-Free]: 1-888-654-9426

United States

United States Secret Service
E-Mail: http://www.ustreas.gov/usss/alert419.shtml
Telephone: 202-406-5850

Federal Trade Commission
Copies of any e-mails that you have received, even if you have not responded, may also be forwarded to the Federal Trade Commission at uce@ftc.gov, for inclusion in the Commission's "spam" database.

Further Information

For further information on "Nigerian letter schemes" or the more recent varieties of Africa-related e-mail solicitations, please consult the following sources:

Government Websites

Royal Canadian Mounted Police, *Nigerian Letter Scam*, http://www.rcmp-grc.gc.ca/scams/nigerian.htm
United States Secret Service, *Nigerian Advance Fee Fraud - "Operation 4-1-9"*, http://www.ustreas.gov/usss/financial_crimes.shtml#Nigerian
Nigerian High Commission in the United Kingdom, *NigerianFraudWatch.org*, http://www.nigerianfraudwatch.org

Publications

Jim Buchanan and Alex J. Grant, *Investigating and Prosecuting Nigerian Fraud*, UNITED STATES ATTORNEYS BULLETIN, November 2001, at 39, reprinted at : http://www.usdoj.gov:80/usao/eousa/foia_reading_room/usab4906.pdf

Issued July 22, 2002